Ottawa, Canada K1A 0P8

GOVERNMENT RESPONSE TO THE SIXTH REPORT OF THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY: "THE RISE OF IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM IN CANADA"

The Honourable Jim Carr, M.P.
Chair
Standing Committee on Public Safety and National Security
House of Commons
Ottawa, ON K1A 0G6

Dear Mr. Carr,

Pursuant to Standing Order 109 of the House of Commons, I am pleased to respond on behalf of the Government of Canada to the recommendations made in the Report of the Standing Committee on Public Safety and National Security titled "The Rise of Ideologically Motivated Violent Extremism in Canada" which was tabled on June 20, 2022.

Since 2014, Canadians motivated in whole or in part by ideological views or grievances have carried out several deadly attacks across the country—causing more casualties than any other form of violent extremism. Events including the 2017 Quebec City mosque shooting, the 2018 Toronto van attack, and the 2020 Toronto Massage Parlour attack underscore the urgent need to address this threat.

In my Mandate Letter, the Prime Minister asked me to work with the Minister of Justice and Attorney General of Canada to bring forward measures to counter the rise of ideologically inspired violent extremism and strengthen the capacity of Canadian police and prosecutors to bring to justice cybercriminals and terror suspects to the fullest extent of the law. I can assure you that addressing this threat is a top priority and officials across the national security and intelligence community are actively working to deliver on this commitment. At the same time, addressing ideologically motivated violent extremism cannot be achieved by national security and law enforcement means alone; it requires a collaborative whole-of-government approach that is transparent and builds trust and understanding through meaningful engagement with Canadians.

As reinforced by the Committee's study and subsequent Report and recommendations, ideologically motivated violent extremism is a cross-cutting societal issue linked to many organizations' mandates and areas of responsibility, including: Digital Safety and Online Harms; Hate and Religious Freedom; Prevention; Protection; Security and Intelligence and Prosecution; Unconscious Biases; and Victims of Violent Extremism.

Taken together, the Government Response highlights what we as a federal government—in concert with provincial and territorial partners, civil society, and others—are doing to address



the rise of ideologically motivated violent extremism in Canada from a whole-of-society perspective. We are committed to keeping Canadians safe from this threat, while respecting their rights and freedoms and privacy protections, and maximizing the positive benefits of modern communications technologies.

Sincerely,

The Honourable Marco E. L. Mendicino, P.C., M.P.

Recommendation 1

That the Government of Canada work with the Provinces and Territories to develop a nuanced, multi-pronged, survivor-centred national strategy to address ideologically motivated violent extremism (IMVE) that includes the following elements:

The Government partially agrees with this recommendation.

Provinces and Territories are important partners in tackling the rise of IMVE in Canada and are engaged in prevention efforts, national security approaches as well as initiatives to address online safety and to combat hate. The Government of Canada continues to engage with Provinces and Territories at the Ministerial, Deputy Minister and Assistant Deputy Minister levels to collaborate and develop approaches to combat IMVE.

IMVE is a cross-cutting societal issue that requires a collaborative whole-of-government, whole-of-society approach that is transparent and builds public trust and understanding through civic engagement. To that end, the Government of Canada is actively working on enhancing its strategic approach to countering IMVE, which is one component of Canada's increasingly complex threat environment. This includes engaging in consultation stakeholders and the Canadian public to ensure that the Government's approach to addressing IMVE is well balanced and reflects the views of a range of stakeholders, including Provinces and Territories.

The Government of Canada places an emphasis on prevention and harm reduction as a way to complement traditional national security, law enforcement, and intelligence responses. Launched in 2017, the Canada Centre for Community Engagement and Prevention of Violence

(the Canada Centre) within Public Safety Canada leads Canada's *National Strategy on Countering Radicalization to Violence* (CRV), including combatting IMVE. The Canada Centre works with all levels of government, not-for-profit organizations, communities, youth, frontline practitioners, academia, law enforcement and international organizations. For example, the Canada Centre co-chairs the Federal/Provincial/Territorial Working Group on Countering Radicalization to Violence, which seeks to identify strategic priorities and increase collaboration and coordination.

The Government of Canada supports survivors and victims of violent crimes. A comprehensive, multi-pronged approach will include consideration of survivors. However, in the field of prevention of IMVE there may not yet be a violent act and survivor. Also, survivors may be individuals who have not committed a violent act but would be considered victims of having been themselves radicalized as a result of exposure and recruitment to IMVE milieus. A comprehensive multi-pronged national strategy will include these varying circumstances, including through prevention.

When perpetrators of violent hate crimes also articulate an underlying ideology or an attempt to affect societal change, hate crimes may cross the threshold into IMVE. Addressing hatemotivated crimes is therefore critical to also addressing IMVE. According to Statistics Canada's 2021 report on police-reported hate crime, hate crimes target the integral and visible parts of a person's identity and may disproportionately affect the wider community. Public Safety Canada's Security Infrastructure Program (SIP) is designed to help communities at risk of hatemotivated crimes by providing funding to make security improvements to community gathering spaces, such as places of worship, educational institutions and community centres.

Similarly to perpetrators of hate-motivated crimes, IMV extremists often victimize marginalized individuals and groups, including women, religious minorities, visible minorities and those belonging to the 2SLGBTQI+ community. For example, IMVE events like the Quebec mosque shooting in January 2017, a terrorist attack which saw six worshippers killed and five others injured at the Islamic Cultural Centre of Quebec City, demonstrated a continued need to protect places of worship for Muslim Canadians to gather safely. Current policies and programs to prevent and counter acts of hate take into account these differential impacts and respond accordingly. Since 2011, the SIP has provided over \$11 million in funding to more than 430 projects across Canada. One hundred and twenty-seven (127) of those recipients were Islamic Organizations, which represents 30% of all contributions. A national strategy on IMVE will be equally sensitive to the differential impacts of acts of extremism by ensuring that measures are taken to support communities at highest risk of victimization.

Recommendations 2, 3, and 4

That the Government of Canada study the feasibility of a regulatory structure to hold platforms accountable for enforcing their terms of service, with measurable metrics to monitor that those standards are being enforced, and which could include the creation of a Digital Safety Commissioner.

That the Government of Canada works with domestic and international partners to identify and remove online bots amplifying extremist content and encourage online platforms to provide contributor and content authentication mechanisms—including web of trust style tools—that enable users to filter content on that basis.

That the Government of Canada works with platforms to encourage algorithmic transparency and reduce online use by terrorist entities by identifying terminology and phraseology for better content moderation decisions.

The Government agrees with these recommendations.

While the Government is responsible for ensuring the safety of Canadians, including in the online space; countering IMVE also requires a whole-of-society approach whereby online service providers and content-sharing platforms play a central role in preventing and addressing this threat.

The November 2021 Speech from the Throne stated that the Government would continue to fight harmful content online. This was reiterated in the December 2021 Minister of Canadian Heritage Mandate Letter where the Minister was directed to "continue efforts with the Minister of Justice and Attorney General of Canada to develop and introduce legislation as soon as possible to combat serious forms of harmful online content to protect Canadians and hold social media platforms and other online services accountable for the content they host. This legislation should be reflective of the feedback received during the recent consultations."

With this in mind, the Government of Canada is designing a new legislative and regulatory framework for online services, including social media platforms. In doing so, it struck an Expert Panel that met weekly for 10 weeks from April to June 2022. The Government of Canada also conducted several stakeholder roundtables across the country, engaged Indigenous organizations, and consulted like-minded jurisdictions. These consultations provided the Government of Canada with considerations on how to move forward with this new legislative and regulatory framework. While the tabling of this legislation will be at a date yet to be determined, the Department of Canadian Heritage is working with other government departments to deliver on this important initiative.

Following the advice received through consultations, the Government of Canada is considering a risk-based approach to platform regulation, whereby online services would be compelled to identify, assess, and mitigate risks on their platforms through their own internal systems and processes. The risks to be identified, assessed, and measured would be set out in legislation.

The Government of Canada notes that many social media platforms have in place terms of service and/or content policies that set out the rules for acceptable user behaviour. However, it is also concerned that these terms of service and/or content policies are not always properly enforced or monitored. To inject transparency and accountability into the systems and processes of platforms, the Government of Canada's preliminary view is that holding platforms accountable through legislation and regulation may provide more effective results.

A new legislative and regulatory framework could include the use of metrics to monitor whether platforms are meeting their obligations to assess and manage risk on their services. These metrics could be informed and measured through regular transparency reporting and auditing to ensure effective enforcement. The Government of Canada is committed to developing a framework for platforms that are backed up by strong enforcement mechanisms.

To administer and enforce this new regulatory structure, the Government of Canada is considering creating a new Digital Safety Commissioner. The Commissioner could be provided with strong audit and enforcement powers to hold platforms accountable to new legislation, including the power to compel information and data from platforms and levy administrative monetary penalties for non-compliance.

The Government of Canada's planned legislative and regulatory framework could target content associated with violent extremism as a risk that platforms must identify, assess, and mitigate. The Government of Canada is aware that bots and bot networks play a role in amplifying this kind of content. Therefore, in holding platforms accountable for the creation and spread of violent extremist content on their services, platforms could be compelled to assess and mitigate the malicious use of bots and bot networks in this context, where applicable, through regulation. However, it is yet to be determined whether the legislation would target bots or bot networks specifically.

The Digital Safety Commissioner could have broad authority to consult and work with domestic and international partners to achieve the goals of the legislation. The Government of Canada has also consulted international partners in the United Kingdom, Australia, and the European Union on developing new legislation, and has discussed the role of bots and bot networks in spreading harmful and illegal content.

The Government of Canada's Expert Panel discussed how the implementation of user controls could have unintended consequences. Some experts asserted that providing users with control over what they interact with could inadvertently aggravate the phenomenon of 'echo chambers' wherein users filter content based on their existing beliefs. This notion becomes especially dangerous in the context of violent extremism, where users can filter for content that further radicalizes and entrenches their beliefs. These situations could arise even when content is filtered based on a set of criteria that emphasizes trusted and verifiable sources—certain users may see such forms of authentication as a reason to distrust these sources further.

With regard to algorithmic transparency, the Government of Canada recently tabled the *Digital Charter Implementation Act* as Bill C-27. This bill includes the *Artificial Intelligence and Data Act*, which introduces new rules to strengthen Canadians' trust in the development and deployment of artificial intelligence systems across the economy. Systems deemed to have a high impact on people would have to meet requirements for assessment and mitigation of risk of harm or bias.

Any organization that manages a high-impact system would be required to publish information in plain language regarding the functioning of the system and measures taken to mitigate the risks associated with it. The Minister of Innovation, Science, and Industry, supported by an

Artificial Intelligence and Data Commissioner, would have broad powers to administer and enforce the Act, including ordering the production of information, third-party audits, or mitigation measures. The Minister would also be empowered to order the public disclosure of additional information.

A key element of the new legislative and regulatory framework for Online Safety could also include transparency requirements, including transparency requirements pertaining to algorithms. The Digital Safety Commissioner could be provided with broad powers to compel data and information from online services.

The Government of Canada agrees that a context-specific and nuanced understanding of terminology and phraseology is essential to addressing the use of online services by terrorist entities. Consistent with the advice provided by the expert advisory group appointed by the Minister of Canadian Heritage and as part of a potential approach to regulating online services based on a duty to act responsibly, platforms would be responsible for mitigating the risk of their services being used by terrorist entities. As part of this risk assessment and mitigation process, services could be required to take into consideration evolving terminology and phraseology when addressing terrorist content through regulation where applicable.

To complement domestic efforts and as part of its international engagement on these issues, the Government of Canada actively participates in the Global Internet Forum to Counter Terrorism (GIFCT), a digital industry body that seeks to address violent extremist and terrorist exploitation of member platforms. The organization fosters technical collaboration among member companies, advances relevant research, and shares knowledge with smaller platforms. Part of this work includes developing technical solutions to prevent/mitigate unintended consequences of the use of algorithms and conducting reviews of the impact of recommender algorithms.

Additionally, the Government of Canada is a signatory to the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online (Christchurch Call), which includes a number of voluntary commitments by governments and digital industry to eliminate violent extremist content online. To help meet these commitments, the Government of Canada, through Public Safety Canada, provided funding to Tech Against Terrorism—a UN-affiliated initiative that supports smaller digital platforms to tackle terrorism exploitation - to develop the Terrorist Content Analytics Platform (TCAP). This resource facilitates the quick and accurate removal of terrorist content by small tech platforms, as the TCAP rapidly provides alerts of verified terrorist material found on their sites or apps.

The Government of Canada also assisted in the development of, and continues to promote adherence to, the Voluntary Transparency Reporting Framework (VTRF) through the Organisation for Economic Cooperation and Development (OECD). The VRTF is a standardized transparency reporting framework that any online content-sharing service can use to report on terrorist and violent extremist content. The transparency metrics include reporting qualitative information pertaining to the use of algorithms to spread and promote violent extremist and terrorist content.

Recommendation 5

That the Government of Canada work with provinces and territories to increase funding for frontline, community-serving organizations—such as the Canada Centre for Community Engagement & Prevention of Violence—whose IMVE programming focuses on prevention through education, intervention, and behavioural health models as well as rehabilitation.

The Government agrees with this recommendation.

Prevention programming to address IMVE delivered through frontline and community services organizations plays a key role in prevention efforts to address IMVE across Canada.

The Canada Centre for Community Engagement and Prevention of Violence (Canada Centre), housed in Public Safety Canada, was established in 2017 to lead the Government of Canada's efforts to counter radicalization to violence (CRV) and all forms of violent extremism, including grievances related to IMVE. Notably, the work of the Canada Centre is complementary to—but distinct from—national security, law enforcement, and criminal justice approaches, recognizing that addressing IMVE is more than an enforcement issue. The Canada Centre works closely with academics, front-line service providers, other federal government departments and agencies, and other levels of government in leading the 2018 *National Strategy on Countering Radicalization to Violence*. A key tool for the Canada Centre's engagement is the Community Resilience Fund (CRF) grants and contributions program, established with \$7 million in annual funding. Budget 2021 provided an additional \$8.2 million over three years.

The Canada Centre supports initiatives and programs to prevent and intervene with individuals and groups at-risk of radicalization to violence, as well as with those who want to leave violent extremism behind. Early prevention initiatives and programs are aimed at the general population and have the objective of preventing the onset of harmful behaviour. One example of an early prevention project that the Canada Centre has supported is The Institute for Strategic Dialogue (ISD)'s Extreme Dialogue. This project developed an educational framework and resources, including guides, films, and testimonies, to support teachers and group facilitators to equip young people with skills to challenge hate and violent extremism in all its forms. Intervention initiatives and programs are directed at individuals or groups in the initial stages of radicalization to violence or who have become directly involved in ideologically motivated violence. One example of an intervention initiative that the Canada Centre has supported is BC Shift, a civilian-led program that works with municipal governments, community-based organizations, and law enforcement to engage vulnerable individuals and develop intervention strategies tailored to them. Yorktown Family Services' Estimated Time of Arrival (ETA) program is another example of an intervention program. ETA deploys rapid, mobile mental health and integrated care for people at risk of radicalization to violence in the Greater Toronto Area. This program targets individuals between the ages of 12 to 35 who might be involved with, at risk of, or present early stages of extremist activity.

The Government of Canada recognizes the importance of adequate and stable funding and capacity building for clinicians, frontline practitioners and community-serving organizations in

order to adequately respond to the increasing demand on their services. This observation has been supported by feedback from the Canadian Practitioners Network for the Prevention of Radicalization and Extremist Violence (CPN-PREV) and member organizations.

The Canada Centre also supports several intervention programs that have established a working relationship with parole officers and the justice system on a case-by-case basis to assist individuals leaving the justice system and reintegrating into the community. Interventions follow a multi-sectoral approach by creating client-centred solutions post release. For example, the CRF-funded research project entitled "Tools for Professionals who Support the Reintegration of Offenders to Detect and Address Radicalization" is receiving funding from the Canada Centre to specifically understand the role of prison chaplaincy in countering radicalization to violence within the incarceration system.

The increased demand on the CRF demonstrates the funding needs of frontline and community organizations. Through its Call for Applications that closed in January 2022, CRF received 130 applications totalling \$170 million, far exceeding the \$6.1 million available for new projects this year (after accounting for commitments already made to multi-year projects). In light of this demonstrated need, the Government of Canada will consider if additional funding for the CRF would be appropriate, noting that the Fund is the largest mechanism in Canada to support investment in intervention programming and in increasing understanding and capacity to prevent and counter violent extremism, online and offline. Priority areas identified include earlier prevention, including online, and threat assessment.

In addition to examining funding levels for the CRF, the Government of Canada will consider needs in the Canada Centre and elsewhere. For example, the Canada Centre could increase its knowledge mobilization and engagement functions, helping to increase networking between academics, front-line service providers and governments, and potentially increase its capacity to undertake analytics, research and behavioural science support.

Recommendation 6

That the Government of Canada convene a summit with the provinces and territories to discuss how existing mental health and social services can better equip and educate front-line practitioners to provide intervention and behavioural health models that address violent and misogynistic movements, while promoting resiliency training.

The Government takes note of this recommendation.

The delivery of mental health and social services is a provincial and territorial responsibility. As such, the Government of Canada recognizes the need to continuously engage with its provincial and territorial counterparts.

The Government of Canada has heard from many practitioners including the Canadian Practitioners Network on Prevention (CPN-PREV) that current funding levels for frontline practitioners are insufficient to address the increasing volume of clients who are at-risk, or

already engaged in, violent extremism.

Public Safety Canada currently consults with federal and provincial and territorial partners, including by co-chairing with the British Columbia provincial government a Federal-Provincial-Territorial (FPT) working group on countering violent extremism (CVE) that includes representatives from all provinces and territories. Recently, members of the CPN-PREV network made a presentation to the FPT working group including to identify resource gaps. Additionally, Public Safety Canada's Canada Centre for Community Engagement and Prevention of Violence has in past years organized a "Megaweek" on CVE, bringing together other levels of government, including provincial, territorial and municipal, along with academics and frontline service providers. Planning has been initiated to organize another "Megaweek" in early 2023, the first since the onset of the COVID-19 pandemic. The Government of Canada will consider whether these existing mechanisms—the FPT working group or Megaweek—would allow for the recommended discussions.

Recommendation 7

That the Government of Canada both acknowledge and protect against the threats posed by violent extremism, including grievance-driven violent extremism, to Canada's critical infrastructure.

The Government agrees with this recommendation.

The Government of Canada is not only dedicated to protecting Canadians from violent extremist threats, but is also committed to protecting critical infrastructure to ensure that Canadians continue to receive essential services.

Canada's National Strategy and Action Plan for Critical Infrastructure sets out an all-hazards risk management approach to strengthening the resilience of Canada's critical infrastructure. This approach takes into account natural, accidental, and intentional threats, such as violent extremism, including grievance-driven violent extremism, that could affect Canada's vital assets and systems. Public Safety Canada offers numerous supports to the critical infrastructure community, including guidance and exercises on insider threats and cyber security as well as physical site assessments. By taking an all-hazards approach, Public Safety Canada and the critical infrastructure community work together to address a range of pathways that could be exploited by threat actors, including those driven by IMVE.

Public Safety Canada is currently undergoing a process to renew the National Strategy for Critical Infrastructure. An all-hazards approach will remain integral to a renewed National Strategy to keep Canada's critical infrastructure resilient for many years to come.

The Royal Canadian Mounted Police (RCMP) continues to work with Public Safety Canada and security and intelligence partners on a strategic approach to address IMVE that would consider resourcing levels to ensure law enforcement agencies can continue to effectively investigate IMVE criminal threats to Canada and Canadians, including acts of violence against persons or

property and threats targeting critical infrastructure.

With respect to cyber threats operating outside of Canada, Communications Security Establishment (CSE) has tools in place to monitor, detect and investigate potential cyber incidents, and to take active measures to address them. CSE's Canadian Centre for Cyber Security (CCCS) encourages the Canadian cybersecurity community—especially critical infrastructure network defenders—to bolster their awareness of and protection against cyber threats. CCCS also shares vital information, including indicators of compromise, to help those critical infrastructure network defenders protect themselves.

With respect to foreign intelligence, this year CSE reported on a range of foreign-based threats including terrorism and IMVE. Reports have noted foreign threat actors from across the ideological spectrum suggesting infrastructure as a possible target for violence/action.

CSE also uses its cyber operations authorities to disrupt and defer the efforts of foreign-based extremists originating online against Canada's interests.

Recommendation 8

The Government of Canada develop legislation using a human rights-based approach to adequately fund and modernize the authorities of Canada's security intelligence community with emphasis on the changing nature of technology and the role played by social media platforms in the evolution of violent extremism in Canada.

The Government agrees with this recommendation.

In Canada, human rights and freedoms are protected by Canada's Constitution and by federal, provincial and territorial legislation. These rights are consistent with those under international treaties to which Canada is a party. It is crucial that these rights and freedoms form the foundation of the Government of Canada's consideration of legislation to fund and modernize the authorities of the security intelligence community.

The Government is studying the existing set of tools available to law enforcement and national security agencies to investigate violent extremism and terrorism online, and is examining the possibility of legislative reforms to modernize these tools online threats represent a modern challenge and demonstrate the need for modernized tools and authorities to protect Canada and Canadians in the digital age. Among other changes being pursued, security and law enforcement agencies may therefore require updates to legislation and authorities that enable data-driven investigations commensurate with the modern and growing threat online.

The Royal Canadian Mounted Police (RCMP) is also analyzing its legislative tools to determine to what extent modernization is required to meet the needs of investigators and analysts operating in the constantly evolving ideologically motivated threat landscape.

Any proposed changes would be designed to achieve objectives in a way that is balanced and proportional, that includes robust safeguards, and that fully respects the privacy rights and

expectations of Canadians.

The Government of Canada is taking action to ensure that threats from violent extremists and terrorists online can be investigated when they use communications platforms based abroad, by negotiating an agreement with the United States consistent with the U.S. *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, and through participation in the recently completed negotiations for the Second Additional Protocol to the Council of Europe Convention on Cybercrime (also known as the Budapest Convention).

The changing nature of violent extremism online has made it vital that investigators can identify, in a timely manner, online actors engaged in criminal activity or that threaten national security. Investigators need access to subscriber information—for example, name and address—that can help identify users of online accounts.

Canada currently lacks a legal framework designed specifically to govern access to subscriber information during the early stages of investigations. The result is processes that are difficult to use, cumbersome, and slow the investigation of online threats at a time when such threats can emerge suddenly.

To address this gap, the Government of Canada will consider possible options for improving regimes for accessing subscriber information, while maintaining appropriately robust safeguards and protections. All potential options, including any legislation, would need to recognize the importance of Canadians' privacy and that any intrusions in this space would need to be reasonable and proportionate by ensuring that the threshold for access to subscriber information is commensurate with the privacy interests at stake.

The RCMP and the Canadian Security Intelligence Service (CSIS) continue to strengthen their intelligence capacity with regard to ideologically motivated threats, including online. Both agencies are working to identify if any additional resources and technical capacity are required to effectively detect threats online, identify criminal actors, and disrupt threats to national security and public safety.

Recommendation 9

That the Government of Canada explore models adopted by other jurisdictions, like the UK and Australia, to implement a made-in-Canada solution to better tackle IMVE and the spread of online hate.

The Government agrees with this recommendation.

IMVE is a serious and emerging challenge faced by Canada and many of its international partners. The Government of Canada can benefit from lessons learned and best practices abroad as it develops and strengthens its domestic approach to combatting IMVE.

The Government is currently designing a made-in-Canada legislative and regulatory framework for online services, including social media platforms, to tackle IMVE and the spread of online

hate. In doing so, it consulted like-minded jurisdictions who have put similar frameworks in place.

The Government of Canada agrees that Canada has much to learn from the experience of other jurisdictions when developing its made-in-Canada solution to IMVE and online hate. To this end, the Government held several meetings with the United Kingdom, Australia, and the European Union at multiple levels of leadership to inform its approach. It will continue to do so throughout both the legislative development and implementation process.

The Government of Canada, through the Canada Centre, also actively participates in international, multi-stakeholder initiatives, such as the Christchurch Call to Action and the Global Internet Forum to Counter Terrorism (GIFCT), to establish best practices for preventing and countering terrorist and violent extremist content online. These initiatives draw upon international governments and digital industry experiences and solutions to reducing the spread of online hate, violence and terrorism. The GIFCT is advised by an Independent Advisory Committee (IAC) made up of representatives from civil society, government, and intergovernmental organizations. The Government of Canada, represented by Public Safety Canada, is one of seven governments on the GIFCT IAC.

The Government of Canada frequently consults other governments on their approaches to IMVE and Violent Extremism more generally, and takes note of their strategies. For example, in February 2022, Australia's Department of Home Affairs announced a \$61 million strategy for Countering Violent Extremism (CVE), including funding for an intervention program, a CVE Community Grants Program, a national program to rehabilitate and reintegrate violent extremists in custody; and an international Centre of Excellence for CVE Research, Risk Assessment and Training. This model is helping inform the Government of Canada's approach to address IMVE from prevention to response, as well as inform possible new investments for Canada.

Recommendation 10

That the Government of Canada invest in its capacity to prosecute the financing of IMVE, while ensuring that terrorist financing laws are properly adapted to capture this threat.

The Government agrees with this recommendation.

Money laundering and terrorist financing threaten Canadians' safety, the integrity and stability of our financial sector, and the broader Canadian economy. Ensuring that Canada has the ability to detect these threats through a comprehensive anti-money laundering (AML)/anti-terrorist financing (ATF) Regime, as well as an equal ability to catch and prosecute these offences, is vital to protecting Canadians and safeguarding the rule of law in an increasingly complex financial world.

The Government is committed to ensuring that its terrorist financing laws continue to be fit-forpurpose and that they provide Canada's investigative, intelligence and prosecutorial agencies with the tools needed to identify, deter and capture the threats Canada faces, including IMVE. In Budget 2022, the Government announced that it will conduct a comprehensive review of its AML/ATF Regime, and will be bringing forward proposals to address identified gaps in the coming months. In addition, as required every 5 years, Parliament will undertake a review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in 2023, to assess the rigour of the legislation. The Government of Canada will also continue to ensure that it has an up-to-date understanding of new and evolving risks pertaining to Canada, such as the exploitation of payment platforms by IMVE actors.

The *Criminal Code's* three terrorist financing offences seek to prevent the financing of terrorism. Broadly, these offences prohibit:

- (a) directly or indirectly providing property intending or knowing it will be used in order to carry out an act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict if its purpose is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act (section 83.02);
- (b) directly or indirectly providing property or making property available intending or knowing it will be used for the purpose of carrying out a terrorist activity, or knowing it will be used by or will benefit a terrorist group (section 83.03); or
- (c) directly or indirectly using property for the purpose of carrying out a terrorist activity or possessing property intending or knowing it will be used directly or indirectly for the purpose of carrying out a terrorist activity (section 83.04).

These offences capture a broad range of conduct, including the financing of IMVE where IMVE falls within the definition of "terrorist activity" in the *Criminal Code*.

The Royal Canadian Mounted Police (RCMP) continues to work with Public Safety Canada and security and intelligence partners on a strategic approach to address IMVE that will address both resourcing and potential legislative gaps that hinder the ability for law enforcement to effectively investigate how IMVE threat actors use funds. Key to this is determining whether or not listed entities are utilizing alternate sources to hide fundraising efforts in contravention to existing Canadian laws. Currently, there is no indication existing terrorist financing laws are insufficient to prevent the RCMP from effectively investigating and laying charges when terrorist financing activities are discovered. The RCMP, along with its security and intelligence partners, is assessing whether or not sufficient resources exist to conduct the comprehensive intelligence work to uncover often complex financing schemes.

Recommendation 11

That the Government of Canada conduct research on the role that crowdfunding, and cryptocurrency play in financing IMVE, while ensuring that the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has the resources and powers necessary to

monitor suspicious transactions made through crowdfunding and cryptocurrency platforms.

The Government agrees with this recommendation.

The Government of Canada is committed to ensuring that it has an up-to-date understanding of the evolving risks of terrorist financing in Canada, including those that relate to the exploitation of crowdfunding and cryptocurrency platforms by IMVE threat actors.

As Canada's financial intelligence unit and anti-money laundering (AML) and anti-terrorist financing (ATF) regulator, FINTRAC is responsible for analyzing, assessing and disclosing designated information pertaining to money laundering and terrorist financing when certain thresholds are met. FINTRAC also ensures the compliance of thousands of businesses with requirements under the *Proceed of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), including financial entities, casinos, money services businesses, real estate and others.

On April 5, 2022, the Government of Canada established new regulations that require crowdfunding platforms and certain payment service providers to register with FINTRAC, develop a compliance program, undertake record keeping, customer due diligence, and report suspicious and large-value transactions. These reporting requirements cover prescribed transactions in both fiat and virtual currency, and apply to domestic entities, as well as foreign entities when they direct their services to Canadians. These new regulations will help mitigate risks that these platforms receive illicit funds; will increase the quality and quantity of information received by FINTRAC; and make more information available to support investigations by law enforcement.

FINTRAC also has a mandate to enhance public awareness and understanding of matters related to money laundering and the financing of terrorist activities. Under the Act, FINTRAC has existing authorities to conduct research into trends and developments in the area of money laundering and the financing of terrorist activities and in improved ways of detecting, preventing and deterring those activities. FINTRAC will continue to conduct research in these areas and undertake measures to inform the public, reporting entities and authorities engaged in the investigation and prosecution of money laundering offences and terrorist activity financing offences on new or emerging financing trends, much as it did with its 2021 Special Bulletin on Ideologically Motivated Violent Extremism. The Department of Finance-led Assessment of Inherent Money Laundering and Terrorist Financing Risks is another way through which the Government conducts research on these topics.

In terms of resources, in Budget 2022, the Government proposed to provide an additional \$89.9M over 5 years and \$8.8M ongoing to FINTRAC. This increased capacity will enable FINTRAC to implement new anti-money laundering and anti-terrorist financing requirements for crowdfunding platforms and certain payment service providers, including to supplement existing resources to ensure compliance, develop tactical financial intelligence and subscribe to the tools necessary to research, analyze and assess trends in this evolving sector. Funding was further provided to complement undertakings related to crowdfunding and payment service

providers, so that FINTRAC can modernize its digital infrastructure and compliance functions as well as continue to build expertise related to virtual currency.

Recommendation 12

That the Government of Canada ensure that terrorist financing laws are properly adapted to capture the rising threat posed by IMVE.

The Government agrees with this recommendation.

The Government is committed to ensuring that its terrorist financing laws continue to be fit-forpurpose and that they provide Canada's investigative, intelligence and prosecutorial agencies with the tools needed to capture the threats Canada faces, including IMVE.

In Budget 2022, the Government announced that it will conduct a comprehensive review of its anti-money laundering AML/ATF Regime, and will be bringing forward proposals to address identified gaps in the coming months. The Government of Canada will also continue to ensure that it has an up-to-date understanding of the evolving risks with a nexus to Canada, including those related to the exploitation of payment platforms by IMVE actors.

The *Criminal Code's* three terrorist financing offences that seek to prevent the financing of terrorism are found in sections 83.02 to 83.04 of the *Criminal Code*. They implement Canada's obligations under the International Convention for the Suppression of the Financing of Terrorism and United Nations Security Council Resolution 1373. These offences capture a broad range of conduct, including the financing of IMVE where the IMVE falls within the definition of "terrorist activity" in the *Criminal Code*. The Government of Canada will continue to monitor the effectiveness of our anti-terrorism regime to ensure it can address the ongoing threats posed by those who would plan or carry out a terrorist activity.

Recommendation 13

That FINTRAC continue to work with provinces and territories and police services of jurisdiction to share information in their mandate and continue to improve communication and collaboration.

The Government agrees with this recommendation.

Information sharing, communication and collaboration are central to the Government of Canada's response to IMVE.

FINTRAC has and will continue to work with provinces and territories and police services of jurisdiction to share tactical and strategic intelligence and information in their mandate, and will continue to improve communication and collaboration. Specifically, FINTRAC shares information with municipal and provincial law enforcement, as well as federal government organizations such as the RCMP, Canadian Security Intelligence Service, Public Safety Canada, Communications Security Establishment of Canada, Privy Council Office, Canada Border

Services Agency, Department of Finance and Department of National Defence.

FINTRAC also shares information with the public and private sector entities as appropriate, as well as international stakeholders such as other financial intelligence units, Five Eyes intelligence agencies, and international organizations like the Financial Action Task Force and the Egmont Group.

Recommendation 14

That the Government of Canada provide additional resources for Statistics Canada to train and work with law enforcement agencies to ensure that hate crime data—on which Statistics Canada should report annually—is consistently collected and comprehensive.

The Government takes note of this recommendation.

The Government of Canada recognizes the need for and importance of reliable and detailed data on hate crime to ensure the safety and inclusion of individuals living in Canada and to inform policy and programming decisions.

Canada is a world leader in terms of police-reported data on hate-motivated crime, but there is always more that can be done to ensure all police services recognize and consistently report hate-motivated incidents within their communities. Almost 20 years ago, Statistics Canada, together with the Canadian Association of Chiefs of Police (CACP), established standardized collection of hate-motivated crimes from police through the Uniform Crime Reporting (UCR) Survey. Each year, Statistics Canada releases the statistics, informing the public of trends in the nature and extent of police-reported hate crime.

Based on the hate crime report published by Statistics Canada in 2021, police reported 2,669 criminal incidents that were motivated by hate. Hate crimes motivated by hatred of a race or ethnicity represented 62 percent of all hate crimes, followed by those targeting religion (20 percent). Collecting this information on motivation helps the Government of Canada accurately assess the threat posed to communities across Canada and tailor approaches to counter hatemotivated crime accordingly. The Government of Canada notes that while witness testimony quoted on page 13 of the Committee's Report indicates that 61 percent of all victims targeted for hate in 2020 were members of religious minorities, there is no police-reported data from Statistics Canada data to suggest this.

Statistics Canada continuously works with police, community organizations and experts to keep pace with the evolving nature of hate-motivated crime and to sustain standardized reporting by police. The UCR survey was most recently updated in 2021 with an expanded list of hate crime motivations and with the option of including more than one motivation. This update expands information on the prevalence of intersectionality among hate incidents, meaning the prevalence of overlapping characteristics which could be the target of hate, such as racialized identity and religion. These changes to the UCR Survey follow two years of consultations with police, community groups and academics. Police must now have more awareness of these new

standards and reporting options. There is therefore a need for Statistics Canada to develop and deliver ongoing training for police across Canada.

Statistics Canada will continue to consider enhancements to the standardized collection of police-reported hate-motivated crimes, including regular and modernized training and incorporating expanded analyses as part of annual data releases. Statistics Canada will also continue working to advance Canada's understanding of the nature of hate-motivated crime, as well as the impacts of the justice system's responses.

Recommendation 15

That the Government of Canada fund research to investigate how extremist organizations are attempting to recruit individuals within the military and police services.

The Government agrees with this recommendation.

The Government of Canada recognizes the importance of evidence-based policy and decision-making and the need to conduct research to better understand how extremist groups operate.

There are several research programs already in place which have been leveraged to investigate how violent extremist organizations are attempting to recruit individuals within the military and police services. This includes the Mobilizing Insights in Defence and Security (MINDS) Program and the Defence and Security Science and Technology (DSST) Program, both housed within the Department of National Defence (DND).

The MINDS Program is designed to facilitate collaboration and mobilize knowledge between DND, the Canadian Armed Forces (CAF), academia, and other experts on defence and security issues. The Program currently funds external research and facilitates expert engagement on hateful conduct and extremism-related policy issues, including preventing radicalization and hateful conduct within the CAF. Since November 2020, "Addressing and Preventing Hateful Conduct and Radicalization" is listed among the priorities against which MINDS applicants are invited to submit proposals. Most notably, through MINDS, DND funds and collaborates with the Right-Wing Extremism in the Canadian Armed Forces Research Network based at Ontario Technical University, in the amount of \$250k/year for 2020-2023. In addition, MINDS has issued various grants for ad hoc projects and events, valued at up to \$50k, on topics related to hateful conduct and radicalization, with recipients in Canada, the United States, the European Union, and elsewhere. MINDS funding has also been utilized to organize briefings from external experts to DND/CAF and Government of Canada audiences on hateful conduct, systemic racism, diversity and inclusion, and other related topics. This ongoing research and funding is critical to investigating how extremist organizations are attempting to recruit individuals within the CAF, and it in turn allows for DND/CAF to better understand its vulnerabilities as an organization and how to protect the institution.

Moreover, under the DSST Program, DND/CAF is conducting research to identify, and counter, extremism influence in the CAF. Through its internal research program and collaboration with

academia and international allies (including through NATO) on hateful conduct, radicalization, and violent extremism, the DSST program seeks to provide evidence-based knowledge to enhance the department's ability to identify prospective and serving members who are potentially on hateful conduct trajectories, and to develop intervention strategies. This includes research on hateful conduct prediction and risk factors, theories of hateful conduct trajectories, radicalization among military members, strategies used by other militaries to detect hateful conduct, extremist groups' motivations to recruit military members, online radicalization, individual propensity, and the role of gender in hateful conduct. The DSST also conducts research to examine the factors related to an individual's susceptibility to being influenced and deceived in the online environment and to explore how violent extremist organizations are using targeted strategies to radicalize susceptible individuals, in order to increase resilience against deception and potential recruitment and radicalization.

Recommendation 16

That the Government of Canada strengthen the internal mechanisms of the Canadian Armed Forces and federal law enforcement in order to hold personnel of these agencies accountable when they are found to be supporting violent extremist movements.

The Government of Canada agrees with this recommendation.

It is crucial that Department of National Defence (DND) and the Canadian Armed Forces (CAF) and federal law enforcement personnel hold themselves to the highest standards of conduct and to ensure their actions are consistent with Canada's core values. DND/CAF along with federal law enforcement agencies, including the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA), have strong internal mechanisms in place to hold personnel accountable should they be found to be supporting violent extremist movements.

DND/CAF do not tolerate hateful conduct in the Canadian military and is committed to detecting, preventing, and addressing extremism within the institution. This sentiment has been stated, and will continue to be reiterated, by the Minister of National Defence and the Chief of the Defence Staff publicly in Parliament, as well as through internal communications to personnel. As such, active steps to address and eliminate hateful conduct from DND/CAF are already underway to strengthen the internal mechanisms at recruitment, retention and career progression to hold CAF personnel accountable when they are found to be supporting violent extremist movements.

The July 2020 Canadian Forces Military Personnel Instruction on Hateful Conduct, which was issued to officers and non-commissioned members of the Regular and Reserve Force, clarifies what constitutes hateful conduct; provides guidance to establish clear expectations with respect to intervention; provides guidance on required training and education to prevent, detect, and respond to hateful conduct; and prohibits hateful conduct in the CAF. DND/CAF recognizes that documents like this must remain evergreen to adequately address all aspects of hateful conduct, which is why the Instruction is already in the process of being updated. As well, the Hateful Conduct Incident Tracking System was implemented in July 2020 to record

responses to alleged incidents which appear "hateful" in nature, which are then investigated. This information will better inform CAF leadership as to how to prevent and eliminate hateful conduct within its ranks. When a determination is made that the incident likely meets the definition of hateful conduct, a spectrum of administrative and disciplinary actions can be taken against the member. Depending on the nature of the incident, subject-matter experts (legal advisors, military police, career administration, etc.) are consulted to determine whether administrative action, disciplinary action, or a criminal investigation is required.

In situations when a DND employee or a CAF member is suspected of supporting ideologically motivated violent extremism, managers or supervisors are expected to report it in accordance with the procedures outlined in National Defence Security Orders and Directives. Depending on the severity of the situation, the report may trigger a more in-depth review as well as the monitoring and reporting of the individual's behaviour by supervisors and/or law enforcement agencies. This can also lead to the initiation of a security review by a multidisciplinary panel, potentially resulting in the revocation or denial of the individual's security clearance or reliability status, and lead to further measures by the member's chain of command concerning future employability in certain trades or within the CAF.

In response to a changing security environment and the addition of known violent right-wing groups to the Public Safety Canada terrorism listing, combined with a rise in hate-motivated incidents, the Canadian Forces National Investigation Service stood up HEDGE (Hateful conduct, Extremism, Drugs and Gang Enforcement) in February 2021. The Canadian Forces National Investigation Service's HEDGE investigates serious and sensitive offences related to hateful conduct, extremism, drug trafficking, and gang enforcement including members of Outlaw Motorcycle Gangs that have a DND/CAF nexus. HEDGE is comprised of 12 Investigators across Canada who receive specialized training in Hateful Conduct, hate and bias crimes, violent extremism, drug trafficking, and gang enforcement techniques to include Outlaw Motorcycle Gangs.

Finally, DND/CAF is also looking at strengthening internal mechanisms to better screen potential recruits, in order to prevent extremism from entering into the ranks. Criminal Records checks are conducted to determine if potential recruits have been charged or convicted of a crime and to review this information to assess suitability for enrolment. Reference checks are also used to help determine whether their character, values and ethics align with those of the Canadian Armed Forces, including screening for affiliation with extremist organizations through visible signs such as clothing or tattoos. As part of Basic Training, new recruits undergo a lesson and self-study package outlining what behaviours constitute hateful conduct, promote positive behaviours, and instruct members on their responsibilities, including how to resolve conflicts and how to access support resources. DND/CAF recognizes that meeting the challenges of an increasingly dangerous and unstable future requires an even more diverse and inclusive CAF, one that is safe from discrimination, hateful conduct, and systemic racism.

Public trust is essential for the RCMP to effectively fulfill its mandate. RCMP members are subject to the same laws as all Canadian residents. In addition, member conduct is guided by

the Code of Conduct of the Royal Canadian Mounted Police.

The objectives of the RCMP Code of Conduct for members are to maintain public trust and promote good conduct, thereby making sworn officers accountable and responsible for their actions. The RCMP Code of Conduct clearly outlines members' responsibilities to conduct themselves in a manner that not only meets, but exceeds, the rightfully high expectations of the public.

The RCMP Code of Conduct applies to all regular members and civilian members both on and off duty, in Canada and abroad. Contraventions of the Code of Conduct are taken seriously and the RCMP is committed to handling conduct issues in a responsive, timely, efficient and fair manner.

The RCMP is also committed to strengthening the trust and confidence of employees, communities, partners and other stakeholders. To this end, the RCMP has commissioned an external review of its Conduct Measures Guide to ensure the measures available, and their application, are appropriate to maintain the confidence of the public, and our employees, in the RCMP.

Phase 1 of the review has been completed and includes findings and recommendations to modernize conduct measures guidance across five key areas:

- Amendments to the Conduct Measures Guide, including regular updates to keep pace with relevant case law and superior court judgments;
- Key considerations for decision makers when deciding on conduct measures;
- Types of decision makers that should decide on allegations of all forms of sexual misconduct;
- Enhanced support and training for decision makers;
- An additional recommendation, outside the scope of the current review, encouraging the RCMP to look at other processes in the current disciplinary framework and modernize as appropriate.

The review will be completed by the end of December 2022. Having a fair, transparent, effective and modern Conduct Measures Guide that holds members accountable for their actions reinforces the RCMP's commitment to building greater trust and accountability with our employees and all Canadians.

The RCMP's staffing policy, applicable to Regular Members (RM), requires Human Resource (HR) managers to review recent conduct history of all RMs being considered for promotion or transfer. Relevant information is obtained from the RCMP Professional Responsibility Sector and, based on a review of this information, the HR manager determines if the member's promotion or transfer will or will not be approved. If an RM had been suspected of, or investigated for hateful conduct, including being found to support violent extremist conduct, it

would be revealed before the staffing transaction was finalized.

All commissioned officer level staffing actions, lateral and promotional, include administrative and conduct checks as part of the succession planning process. If an officer had been suspected of, or investigated for hateful conduct, including being found to support violent extremist conduct, it would be revealed before the staffing transaction was finalized.

RM recruitment is essential to the RCMP's ability to meet its service delivery commitments under the provincial, territorial and municipal police service agreements, and to maintain federal policing capacity. It contributes to the achievement of the RCMP's strategic outcome of a safe and secure Canada through the delivery of trained and operational RCMP Regular Members. The RCMP RM recruitment process is very thorough and consists of various screening tools to ensure that all applicants exemplify the RCMP's core values and meet the same high standard of suitability. In order to apply as a police officer with the RCMP, applicants must pass rigorous suitability, medical and security screening protocols. At various stages during the recruiting process, the RCMP's trained recruiters look at each applicant's situation and make their determinations based on the recency, frequency and severity of an applicant's behaviour or concerns. These precautions and measures are taken to ensure public confidence in the RCMP. As each RM applicant's experiences and past behaviours are different, applicants are assessed on a case-by-case basis.

In addition to its robust recruitment process, the RCMP employs an enhanced security screening program, which includes criminal record checks, financial inquiries, open source queries, a security interview/questionnaire and law enforcement records checks. Security screening is a fundamental practice that establishes and maintains a foundation of trust within government, between government and Canadians, and between Canada and other countries. This process is continuous in nature and regularly renewed during an employee's career depending on their role within the organization. Should allegation arise that an employee is supporting ideologically motivated violent extremism, those allegations will be reviewed and, if warranted, may result in a security review for cause investigation, which could result in the revocation of an employee's security clearance or reliability status. It is important to note, the security screening process is applicable to all employees and to contractors (when required).

Ultimately, the totality of the tools and policies within the RCMP assist in mitigating the risks associated to IMVE and will continue to be enhanced to ensure the integrity of the organization's employees with respect to all threats which may negatively impact on the RCMP's ability to achieve its mandate.

Lastly, the CBSA is committed to upholding the highest professional standards in accordance to Canadian values, ensures that employees are aware these expectations, and has a robust and comprehensive framework and mechanisms to address when behaviour does not meet expectations, including but not limited to supporting violent extremist movements. The CBSA works with law enforcement partners as appropriate, within the bounds of applicable privacy legislation.

The Agency has a robust security screening program to identify any potential security concerns for all applicants to CBSA positions. All CBSA law enforcement positions require an Enhanced Reliability Status and a Secret clearance (at a minimum), which includes verification of online activities, law enforcement records and verification with the Canadian Security Intelligence Service. Applicants found to have links to IMVE would be considered a security risk to the CBSA and would see their requested status or clearance denied. Furthermore, all frontline officers must undergo a Law Enforcement Records Check, a service provided by the RCMP to the federal public service.

In addition, the CBSA Code of Conduct provides guidance on employee responsibilities and the standards of conduct expected. It provides employees with concrete examples on when to report a potentially problematic situation (e.g. relatives involved in criminal activities, being offered a benefit to assist in cross-border movement, and being approached by a known/suspected criminal in a social setting). To complement the Code of Conduct, the CBSA has developed and implemented the Disciplinary Measures Framework to ensure a high standard for employee conduct, promote a shared understanding of misconduct and possible consequences, and provide a fair, consistent, and transparent approach for addressing misconduct.

Furthermore, all CBSA employees must undertake mandatory training courses related to: Security Awareness; Values, Ethics and Disclosure of Wrongdoing; Values and Ethics Foundations for Employees (and for Managers); Insider Threats (a course that is designed to deter, detect, and mitigate actions by insiders who represent a threat to national security). The CBSA Office of Values and Ethics (OVE) also offers monthly sessions to all CBSA employees to address a variety of topics, such as conflict of interest, respect for democracy, integrity, and stewardship. Dedicated sessions are also offered to all employees related to social media, and the risk factors associated with its use. All training emphasizes the importance of effective use of assets and resources and the importance of ensuring that confidential or privileged information that employees have access to in the course of their work at the CBSA remains confidential.

All allegations of employees with potential links to IMVE would undergo a formal investigation within the CBSA. The investigation serves to determine the facts, and come to a conclusion as to whether the allegations are founded or not. It serves as a basis upon which management can rely on to take decisions on corrective measures, which could include discipline up to and including termination. In addition, from a security screening perspective, a security status or clearance holder found to support IMVE would be a clear security concern, both from a reliability perspective and a loyalty to Canada perspective. Such information may result in the revocation of the employee's security status or clearance, which is a condition of employment for all positions within the CBSA.

Recommendation 17

That the Government of Canada consult with the survivors of IMVE to ensure that support and response systems reflect survivors' needs.

The Government takes note of this recommendation.

Addressing the needs of victims and survivors of crime as well as making the criminal justice system more accessible, efficient and effective are priorities for the Government of Canada. The Government of Canada is committed to ensuring that victims of crime, their families and their loved ones, are treated with courtesy, compassion, and respect throughout the criminal justice system and will continue to work to address their needs, including in collaboration with the provinces and territories.

The responsibility for victims of crime is shared by the federal, provincial, and territorial governments. Under the Canadian Constitution, the federal government is responsible for the development of criminal law and procedure, much of which is set out in the *Criminal Code*. The federal government also conducts the prosecution of *Criminal Code* offences in the territories.

Provinces and territories, however, are principally responsible for the administration of justice, which includes the delivery of victim services and enacting victim legislation at the provincial and territorial level. Each of the provinces and territories has enacted victim legislation that establishes their victim service programs and compensation schemes, where they exist. The provinces and territories determine how these programs will be administered. Each jurisdiction has chosen a model that best suits their respective province or territory.

Recommendation 18

That the Government of Canada establish a domestically focused counterpart to Global Affairs Canada's Office of Human Rights, Freedoms and Inclusion, ensuring that this new office is appropriately resourced and embraces a multi-faith approach in its efforts to protect and report on religious freedom and acceptance in Canada.

The Government takes note of this recommendation.

The Government of Canada is committed to the promotion and protection of freedom of religion or belief, both at home and around the world and is actively working to combat hate, racism and discrimination, including that based on religion or belief.

While Global Affairs Canada's Office of Human Rights, Freedoms and Inclusion (OHFRI) leads Canada's international policy development and advocacy on issues related to human rights, the Government is continuously engaged in a number of domestically focused initiatives aimed at protecting and supporting religious freedom in Canada. One of Canadian Heritage's (PCH) portfolio organizations, the Canadian Race Relations Foundation (CRRF), is committed to building a national framework for the fight against racism in Canadian society. The Government

provided financial support to CRRF through Budget 2021 to scale up efforts to empower racialized Canadians and help community groups combat racism in all its forms.

In 2019, the Government launched *Building a Foundation for Change: Canada's Anti-Racism Strategy 2019–2022*. The Strategy is based on three guiding principles: demonstrating federal leadership, empowering communities and building awareness and changing attitudes. Along with a suite of funded initiatives, the Strategy established the Federal Anti-Racism Secretariat, which leads work across the Government of Canada to coordinate federal action, engage with diverse communities across Canada and report publicly on whole-of-government outcomes.

The Strategy committed to strengthen the Government's capacity to combat racism and hate by investing close to \$100 million, including \$70 million to support community organizations across Canada through two funding streams: the Anti-Racism Action Program, which supports multi-year projects that address barriers to employment, justice and/or social participation, and; the Community Support, Multiculturalism and Anti-Racism Initiatives Program, which provides funding for community development, anti-racism initiatives, and engagement projects.

PCH is actively leading work on a new Anti-Racism Strategy and National Action Plan on Combatting Hate. To support the new Strategy, Budget 2022 proposes to provide \$85 million over four years to support community projects that ensure that Black and racialized Canadians and religious minorities have access to resources that support their full participation in the Canadian economy, while also raising awareness of issues related to racism and hate in Canada.

In July 2021, the Federal Anti-Racism Secretariat introduced a National Summit on Antisemitism and a National Summit on Islamophobia to hear input from Jewish and Muslim communities to inform the new National Action Plan on Combatting Hate. Both summits were attended by community leaders, Prime Minister Justin Trudeau, federal ministers, members of Parliament and officials from provincial and municipal governments.

Recommendation 19

That the Government of Canada expand the Special Envoy on Preserving Holocaust Remembrance and Combatting Antisemitism's mandate to include more educational awareness on the Holocaust.

The Government takes note of this recommendation.

Antisemitism and hate have no place in Canada, and counter to the values and spirit of a diverse and inclusive society. At the Malmö International Forum on Holocaust Remembrance and Combating Antisemitism on October 13, 2021, Prime Minister Trudeau pledged to "expand publicly accessible Holocaust-related material and to bring awareness to the dangers of antisemitism," including, "by using the historical legacy of Raoul Wallenberg - Hero of the Holocaust and Canada's first honorary citizen - as an inspirational role model for educational purposes."

Building a Foundation for Change: Canada's Anti-Racism Strategy 2019–2022 introduced a Special Envoy for Preserving Holocaust Remembrance and Combatting Antisemitism, to advance the Government's work on combatting antisemitism at home and abroad and preserving Holocaust remembrance. Canada's Special Envoy is also Head of Canada's Delegation to the International Holocaust Remembrance Alliance (IHRA), which works to combat antisemitism and to strengthen, advance, and promote Holocaust education, research and remembrance. In November 2021, the Government reappointed Professor Irwin Cotler to a second term in the role.

Budget 2022 proposes to provide \$5.6 million over five years and \$1.2 million of ongoing funding to support the Special Envoy. Beyond the role of the Special Envoy, Budget 2022 provides a \$20 million commitment in 2022-23 to Canadian Heritage to support the construction of the new Holocaust Museum in Montreal, as well as its investment of \$2.5 million for the Sarah and Chaim Neuberger Holocaust Education Centre.

Between November 2020 and January 2022, Global Affairs Canada's OFHRI has dedicated \$3.5M to projects addressing antisemitism as part of its broader mandate. This funding has supported work with international partners including UNESCO, the United States Holocaust Memorial Museum and the Organization for Security and Co-operation in Europe to support training, education and outreach efforts.

Recommendation 20

That the Government of Canada thoroughly reject the demonization and delegitimization of the State of Israel, and condemn all attempts by Canadian organizations, groups, or individuals, including university campus associations, to promote these views, both at home and abroad.

The Government takes note of this recommendation.

Canada has been a steadfast friend and ally of Israel since 1948 and is proud to have been one of the first countries to recognize the State of Israel. Support for Israel, especially its right to live in peace and security with its neighbours, has been at the core of The Government of Canada's Middle East policy since 1948.

The Government of Canada is concerned by efforts, such as Boycott, Divestment and Sanctions (BDS), to single out Israel for criticism and isolate Israel internationally. Parliament clearly expressed its concern for the BDS movement when the House of Commons voted in large majority, on February 18, 2016, for a motion rejecting the movement. The Prime Minister reaffirmed Canada's concerns when he condemned the BDS movement during the April 2019 state visit by the President of Israel, and the May 7, 2019, National Holocaust Remembrance Day Ceremony in Ottawa.

The Government also recognizes that manifestations of demonization and delegitimization could be regarded as anti-Semitic when it targets the State of Israel, conceived as a Jewish

collectivity and denies the Jewish people their right to self-determination. To this end, as part of Canada's national Anti-Racism strategy, Canada has adopted the International Holocaust Remembrance Alliance's (IHRA) working definition of antisemitism and has committed to promoting it internationally. In Budget 2022 Canada is investing \$5.6 million over 5 years and \$1.2 million ongoing to support the mandate of the Special Envoy for Preserving Holocaust Remembrance and Combatting Antisemitism. In October 2021, the Prime Minister pledged to make the Special Envoy a permanent position with dedicated funding.

The Government has also taken other steps to fight antisemitism domestically. For example, a National Summit on Antisemitism was held in July 2021 and gave an opportunity to Jewish communities to share their lived experiences of antisemitism and provide input and feedback to inform Canada's first ever National Action Plan on Combatting Hate and a new Anti-Racism Strategy. Prime Minister Justin Trudeau, ministers, community leaders, and officials across all levels of government were in attendance.

Budget 2022 provides a \$20 million commitment in 2022-2023 to PCH to support the construction of the new Holocaust Museum in Montreal as well as an investment of \$2.5 million for the Sarah and Chaim Neuberger Holocaust Education Centre. These two institutions will continue being instrumental in raising awareness on the Holocaust and fighting antisemitism. Recognizing that Canada's fight against racism is far from over, Budget 2022 further proposes to provide \$85 million over four years, starting in 2022-2023, to Canadian Heritage (PCH) to support the work underway to launch the new anti-Racism Strategy and a National Action Plan on Combatting Hate.

Lastly, through Budget 2022, the Government proposes to amend *the Criminal Code* to prohibit the communication of statements, other than in private conversation, that willfully promote antisemitism by condoning, denying, or downplaying the Holocaust.

Recommendation 21

That the Government of Canada appoint a special envoy on Islamophobia.

The Government takes note of this recommendation.

The Government of Canada recognizes that Islamophobia is a concrete and daily reality for Muslim communities across Canada and around the world, and is committed to taking concrete action to address Islamophobia in all its forms.

At the National Summit on Islamophobia in July 2021 hosted by Canadian Heritage, the Government of Canada heard input from Muslim communities to inform the new National Action Plan on Combatting Hate. The appointment of a special representative was one of the recommendations put forward during the Summit.

On June 6, 2022, Minister Hussen announced the launch of the Notice of Appointment Opportunity for the first Special Representative on Combatting Islamophobia. The Special

Representative will serve as a champion, advisor, expert, and representative to the Canadian government, for the purpose of enhancing efforts to combat Islamophobia and to promote awareness of the diverse and intersectional identities of Muslims in Canada. The Special Representative will collaborate with domestic partners, institutions and stakeholders to support Canada's efforts to combat Islamophobia, anti-Muslim hate, systemic racism, racial discrimination and religious intolerance. Eligible candidates were encouraged to submit their applications by July 6, 2022.

To push back against religious discrimination, hateful rhetoric and racism at home and abroad, Budget 2022 proposes to provide funding to support the mandate of the new Special Representative on Combatting Islamophobia. In recognition of the importance of remembrance in supporting public education and combatting hate, the Government of Canada also established the first National Day of Remembrance of the Quebec City Mosque Attack and Action Against Islamophobia on January 29, 2022.

Recommendation 22

That the Government of Canada work with the provinces and territories to develop best practices aimed at countering and investigating IMVE, hate crimes and online hate.

The Government agrees with this recommendation

The nature of the ideologically motivated threat landscape—including IMVE, hate-motivated criminality, and online hate—raises jurisdictional and mandate considerations that enhance the need for coordination and information sharing between different levels of law enforcement and the security and intelligence community.

Pursuant to the *Security Offences Act*, the Royal Canadian Mounted Police's (RCMP) Federal Policing National Security Program has primary responsibility to investigate IMVE criminal activity that rises to the level of a national security threat as defined in section 2 of the *CSIS Act*. IMVE national security criminality can include terrorist activity and terrorism offences within the meaning of the *Criminal Code*, as well as any other offence arising out of conduct constituting a threat to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* (primarily sections 2[c] and 2[d]). The RCMP maintains close partnerships with the Canadian Security Intelligence Service (CSIS) and other domestic security and intelligence agencies, and engages in tactical information sharing with foreign partners to counter IMVE threats.

Police of jurisdiction have primary responsibility to investigate criminal activity that falls short of the national security threshold. It can be difficult to determine whether criminal activity meets the national security threshold at the outset of an investigation or based on an intelligence lead, which highlights the importance of law enforcement coordination at all levels on IMVE and hate crime investigations, including in the online space. RCMP Federal Policing works closely with provincial and municipal police forces on a regular basis, including through the Canadian Association of Chiefs of Police, to identify criminal threats of national security

interest and conduct coordinated investigations.

The RCMP provides contract policing services to all provinces and territories (P/T), with the exception of Ontario and Quebec, as well as to some 155 municipalities. These services are provided through Police Services Agreements, which see the costs for RCMP services shared by the provincial or municipal government, and the federal government. In consultation with the RCMP, P/Ts and municipalities establish the level of resources, budget and policing priorities in their respective jurisdictions. As such, further enhancement or augmentation of programming, including priority level and commensurate resourcing, to develop best practices aimed at countering and investigating IMVE, hate crimes and online hate on the part of front-line police, would need to be determined in consultation with the contract jurisdictions.

Hate crimes, which have widespread negative impacts on individuals and communities, are on the rise in Canada. A Hate Crime Task Force co-chaired by the RCMP and the Canadian Race Relations Foundation has been established by the Chiefs of Police National Roundtable, with policing and government representatives from across Canada. The Hate Crime Task Force will work together to increase the awareness of the scope, nature and impact of hate crimes and to create national standards to better support impacted communities across the country. It will concentrate on topics such as improving communication to the public, creating a network of hate crime units, enhancing hate crime reporting, reviewing police training, and supporting hate crime prosecutions.

Recommendation 23

That the Government of Canada increase research funding to better understand and counter the operational tactics and societal impacts of all forms of IMVE—including xenophobic violence, anti-authority violence, gender-driven violence, and other grievance-driven or ideologically motivated violence.

The Government takes note of this recommendation.

The Government of Canada is committed to supporting research, including on social aspects of IMVE, to ensure that its response to this issue is comprehensive and gender-informed. The Canada Centre for Community Engagement and Prevention of Violence housed in Public Safety Canada (the Canada Centre) leads the Government of Canada's efforts to counter radicalization to violence and all forms of violent extremism, including grievances related to IMVE. The work of the Canada Centre is complementary to—but distinct from—national security, law enforcement, and criminal justice approaches. Greater emphasis is placed on prevention and harm reduction, similarly to fields like community safety and well-being, social work, public health, and conflict resolution.

The Canada Centre supports funding both prevention programming and related research, through the Community Resilience Fund (CRF), a federal grants and contributions program managed by Public Safety Canada. The CRF has a core budget of \$7 million per year, and provides financial support to organizations working to improve Canada's understanding and

capacity to prevent and counter violent extremism. Examples of CRF funded research related to understanding societal impacts include; an innovative partnership between Ontario Tech University and the United Kingdom's Institute for Strategic Dialogue (ISD), to examine the beliefs, motivations, activities, and connections that characterize IMVE milieus in Canada, online and offline. Another is led by Moonshot on 'Improving Knowledge and Research Capacity on the Global Intel Community and its Canadian Impact.'

The 2021 CRF Call for Applications, included as one of its priorities "Locating harm, vulnerabilities and needs", to increase the evidence base on vulnerabilities, risks and pathways to violence, to better inform prevention efforts, including to IMVE. For the 2021 Call, Public Safety Canada received 130 applications totalling \$170 million. A number of proposals were received to help promote understanding about the nature and threats from IMVE, including to inform front-line practitioners, such as social workers, mental health professionals, or police officers. The 2021 call saw the highest number of applications to the CRF ever, seeking funding well above the capacity of the program.

While such prevention-focused research projects can and do contribute to awareness and training of law enforcement, as well as from sectors like social work and clinical health, they are not focused on operational questions that fall under the mandates of police, or security intelligence agencies.

The RCMP supports the funding of research to better understand and counter the operational tactics and societal impacts of all forms of IMVE—including xenophobic violence, anti-authority violence, gender-driven violence, and other grievance-driven and ideologically motivated violence. However, the funding should be reserved for credible subject matter experts, field practitioners and academics with knowledge of the IMVE space.

Recommendation 24

That the Government of Canada work with the provinces and territories —in consultation with IMVE survivors—to ensure police of jurisdiction receive training on IMVE, hate crimes, and online hate, while supporting provincial police forces in their operations to infiltrate extremist circles and groups.

The Government agrees with this recommendation.

The Government recognizes the need to properly train its law enforcement personnel, not only at the time of recruitment, but also throughout their careers to ensure they are able to keep Canadians safe.

At the time of recruitment, cadets learn the foundations of policing, such as *Criminal Code* offences, Arrest and Release Procedures, Firearms, Police Defensive Tactics, Driving, and Physical Fitness with the expectation of growth, continued learning and development in the field, including through training on IMVE, hate crimes, and online hate. Prior to COVID-19 pandemic, the RCMP was in the process of augmenting IMVE training to all its members

working in the field, however, many of these training opportunities did not materialize given the limitations to deliver classroom training during the pandemic. Over the past several months, the RCMP has begun the process of revamping its IMVE training programs and will be offering both introductory and advanced training on IMVE going forward. This training has been specifically designed to incorporate elements that directly relate to both Police of Jurisdiction (POJ) (provincial, territorial and municipal), as well as material that benefits prosecutors. The intent of these training programs is to offer them to POJs as well as provincial and federal prosecutors.

With respect to assisting provincial police forces in operations to infiltrate violent extremist groups, it is important to understand that the RCMP's Federal Policing Program has primary jurisdiction when it comes to investigating ideologically motivated criminal threats to Canada's national security, as defined by section 2(c) of the *CSIS Act*. The RCMP works collaboratively across the organization, in both a Federal Policing role and as the POJ across much of Canada. Further, it works closely with provincial police forces to support the work being done to infiltrate IMVE criminal networks.

At the federal level, the RCMP is working to increase internal capacity for intelligence activities in the IMVE space. Increasing capacity at the provincial, territorial and municipality level, is at the discretion of the respective jurisdiction and appropriate level of government.

In addition, the Public Prosecution Service of Canada is committed to working with the RCMP and other police services to provide training and ongoing advisory support in respect of the applicable legal framework for the various offence provisions and the impact of investigative steps and evidence gathering approaches on prosecutions and the ability to proceed with charges.

The Hate Crime Task Force, co-chaired by the RCMP and the Canadian Race Relations Foundation, will be focused on increasing awareness of the scope, nature and impact of hate crimes across Canada and to create national standards to better support targeted communities across the country. This will include police training, effective engagement with victims and communities, and supporting hate crime units across the country.

Task force participants currently represent 11 police services across Canada with a range of experience and expertise, including working in frontline policing, outreach and engagement, hate crime units, victims' services, and training and education. It is anticipated that additional police services will join the task force over time. One initial topic of interest for the task force includes reviewing and identifying opportunities to update police training.

The Canadian Police College's (CPC) Technological Crime Learning Institute (TCLI) further supports the training of skills needed to investigate online hate and gather evidence from open Internet and DarkWeb sources through its offerings of the Using the Internet as an Intelligence Tool (INTINT) and the Advanced Open Source Intelligence Course (AOSINT) courses. These courses are available to RCMP investigators as well as investigators from other police services

and law enforcement agencies.

Recognizing that there is existing training at the CPC, the RCMP will work to align with existing learning curriculum in support of IMVE. A training gap analysis will enable the identification of the knowledge, skills and abilities (KSAs) required to support IMVE, and the development of subsequent corresponding training curriculum for frontline police officers, up to advanced and specialized training.

Recommendation 25

That the Government of Canada ensure that the RCMP, national security agencies and the Public Prosecution Service of Canada have adequate resources to investigate and prosecute offences against Canada's critical infrastructure and personnel, and ensure Canada's antiterrorism laws are applied equally.

The Government agrees with this recommendation.

The Government of Canada recognizes that a robust toolkit and resource levels commensurate with the threat environment are required to counter IMVE, including threats to critical infrastructure and personnel. Canada has a comprehensive counter-terrorism and criminal legislative framework which includes a suite of tools to identify and disrupt threat actors. These include: investigations that may support criminal charges; terrorism peace bonds; no-fly listings; the revocation of passports; and terrorist listings.

Nonetheless, the Government continues to evaluate the effectiveness of its existing tools to identify areas for improvement and plan for new investments, to ensure that they are fit for purpose. The Government also continues to assess resource needs for the security and intelligence community in relation to the ideologically motivated threat landscape, to ensure its agencies and prosecutorial services have the means to fulfill their mandates.

Government of Canada institutions take care to ensure a balanced approach to investigations and prosecutions, and have embedded robust mechanisms for accountability, oversight and review. Canada's counter-terrorism efforts are governed by laws and policies consistent with the Constitution and the *Canadian Charter of Rights and Freedoms*, and will continue to be applied under guidance of these principles.

Recommendation 26

That the Government of Canada establish a Financial Crimes Agency and equip it with the means to investigate and identify financing of IMVE to cut off its funding at the source.

The Government takes note of this recommendation.

The Government of Canada recognizes the serious threats financial crimes pose to the safety, security and prosperity of all Canadians and is committed to establishing a new Financial Crimes

Agency, mandated to investigate these complex crimes. In Budget 2022, the Government is providing \$2 million to Public Safety Canada in 2022-2023 to undertake initial work to develop and design the new agency. As these efforts get underway, the Government will carefully consider all options to ensure the new agency's mandate ultimately supports its investigative and enforcement effectiveness in this space. Further details will be provided in the 2022 fall economic and fiscal update.

Budget 2022 also provided \$89.8 million over five years and \$8.8 million ongoing to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to implement new Anti-Money Laundering/Anti-Terrorist Financing requirements for crowdfunding platforms and payment service providers, enhancing the financial intelligence necessary to investigate and identify the financing of IMVE.

The Canadian Police College (CPC) offers a Financial Investigations Course which provides investigators with the tools to collect and preserve evidence in order to successfully prosecute individuals involved in financial crimes. It focuses on the recognition of crime associated with capital market manipulation, security fraud schemes, mass marketing fraud, cybercrime, identify thefts, terrorist financing and other types of fraud, and the laundering of proceeds of crime (money laundering). Training provided by the CPC would contribute to the ability of investigators in the new agency to carry out their functions.

Recommendation 27

The Government of Canada, in recognition of the need to address the rise in hate crimes and violence targeting religious communities and places of worship, provide increased funding for the Communities at Risk: Security Infrastructure Program and enhance it to be more effective, accessible, and responsive to community needs, including through expanded eligibility criteria and a simplified application process.

The Government takes note of this recommendation.

The Government of Canada is committed to ensuring Canadians feel safe to gather in their communities, particularly those who face racial and religious intolerance. Public Safety Canada's Communities at Risk: Security Infrastructure Program (SIP) helps protect those at risk of hate-motivated crimes by providing private, not-for-profit organizations such as places of worship, schools, and community cultural centres with funding to enhance their security infrastructure. To demonstrate that commitment, the federal government recently increased the funding available for the Program: Budget 2021 announced a one-time investment of \$2 million in 2021-22 to respond to an increase in hate-motivated crime against Asian Canadians during the COVID outbreak. This investment builds on the 2020 Fall Economic Statement which provided \$13 million over 5 years and \$2.6 million ongoing to the program.

The 2021 Minister of Public Safety Mandate Letter includes a commitment to exploring potential adjustments to the Security Infrastructure Program to enhance effectiveness and to be more responsive to community needs, in support of the development of a National Action

Plan on Combatting Hate led by the Minister of Housing and Diversity and Inclusion. Subsequently, Public Safety Canada, in consultation with the Federal Anti-Racism Secretariat at Canadian Heritage, hosted a series of virtual meetings with members of the Asian-, Muslim- and Jewish-Canadian communities across Canada to obtain feedback on how the Program can be adjusted to be more responsive to their needs, and inform any next steps by the Department.

One example of a modification that has already been implemented, in order to respond to community feedback, has been the extension of time allowed to implement projects. Previously, applicants had 12 months to complete projects, but that has been expanded to 18 months if required. This change removes a degree of pressure felt by organizations to work around Canada's limited construction seasons. Public Safety Canada is also seeking to clarify communication with applicants and organizations to provide better support on the application process, as well as to counter misconceptions about the program. For example, there is no requirement for an organization or the project site to have been a direct victim of a hate crime in order to apply and be successful under the standard call for applications.

Recommendation 28

That the Government of Canada remove the need to demonstrate risk for applicants to apply to the Communities at Risk: Security Infrastructure Program and create a fast track for communities at greatest risk.

The Government partially agrees with this recommendation.

The Government of Canada recognizes that not all communities face the same level of risk and that flexibility in approach may be warranted. The objective of the Communities at Risk: Security Infrastructure Program is to support communities at risk of hate-motivated crime. By demonstrating risk, the Department ensures that only those communities in need are funded and ensures that the limited funding is directed to those organizations with the most pressing need, allowing the government to better support potential victims of hate crime, for which few programs exist.

Public Safety Canada agrees with the recommendation to create a fast track for communities at greatest risk; however, removing the input from applicants regarding their risks and vulnerabilities would, in fact, hinder the Department's ability to identify applicants at greatest risk.

Additional modifications to the Program are also being considered to reduce delays, including providing direct support to communities in times of crisis after a major hate-related attack.

Recommendation 29

That the Government of Canada improve the Communities at Risk: Security Infrastructure Program to expand the eligibility criteria to include funding for non-physical security infrastructure.

The Government takes note of this recommendation.

The Government of Canada recognizes that threats facing communities go beyond physical infrastructure. In light of the feedback received from community stakeholders during consultations in 2021 on the existing Security Infrastructure Program design, Public Safety Canada has identified a number of opportunities to eliminate barriers for participation and identify areas where the eligibility could be expanded to include additional at-risk recipients and protection measures/activities. This analysis is ongoing and will include the Committee's findings and input for consideration.

Recommendation 30

That the Government of Canada create a national digital media literacy strategy that funds digital literacy programs to build Canadian's critical and civic media consumption skills across the entire population, including how to identify conspiracy theories, disinformation and misinformation online.

The Government takes note of this recommendation.

The Government agrees that civic digital literacy is crucial in addressing the creation, spread, and impact of online mis- and disinformation. The Government has made it a priority to help equip citizens with the tools and skills needed to critically assess online information, including as part of the Government's plan to protect democracy and safeguard our democratic processes, which was established prior to the 2019 federal election and renewed for 2021 and beyond.

To that end, the Government funds digital literacy programs through the Department of Canadian Heritage's Digital Citizen Contribution Program (DCCP) which supports the priorities of the Digital Citizenship Initiative (DCI). The DCI is a multi-component strategy that aims to support democracy and social inclusion in Canada by building citizen resilience against online disinformation and building partnerships to support a healthy information ecosystem.

Created in 2019, the DCCP has funded 46 projects with \$7 million to date to build citizen resilience to online disinformation across Canada through workshops, resources for educators, awareness activities, training tools, learning materials, and community outreach. These projects seek to build the critical and civic media consumption skills required to navigate the online information ecosystem for all Canadians. Digital literacy projects funded through the DCCP have resulted in 170 unique events and reach an average of 1.5 million Canadians.

Eligible applicants to the program include not-for-profit organizations, universities or educational institutions; individual researchers acting in their personal capacity; research institutions with established records in relevant fields undertaking work in a Canadian context; and for-profit Canadian and Canadian owned institutions with a record of developing and

delivering programming, and performing research or related activities relevant to the goals of the DCI, provided that the nature and the intent of the activity is non-commercial.

Each year, the DCI reassesses its focus through consultations with a steering committee of experts in the field of online harms and disinformation. The DCI then adapts its priorities and guidelines to adapt its funding strategy to the ecosystem's needs and address the evolving gaps. To this end, the DCCP has funded projects that have been: nationally, regionally or locally focused; in English, French and/or other languages; aimed at minority communities, Indigenous communities, youth, and/or older Canadians.

The DCCP's previous research project calls for proposals sought to fund projects that aim to:

- map/predict the next issues and/or types of online disinformation;
- further understand the impact of disinformation on diverse and marginalized communities in Canada;
- better understand the societal factors and psychological characteristics that motivate individuals to take up the call for online and offline disinformation-related activities;
- understand the impacts of a lack of exposure to diverse content online, including understanding how users access reliable news and information in Canada, as well as the impacts of algorithmic systems on the content users are exposed to and consume on online platforms;
- understand the role of algorithms, artificial intelligence, and other system-level factors on mainstream and fringe online platforms as they pertain to the spread, uptake, and impacts of disinformation and related harms, including on user behaviour and content consumption, and their potential uses towards a diverse and healthy information ecosystem;
- understand the domestic and transnational spread, evolution, and impacts of online disinformation and related harms through and on diaspora, Indigenous, and non-English primary language communities in Canada using a GBA+ lens, including impacts on societal outcomes;
- evaluate existing Canadian or international research and programming related to online disinformation and their effectiveness in furthering positive societal outcomes, such as citizen resilience, social cohesion, media literacy, and participation and trust in democratic processes;
- evaluate the efficacy of efforts by platforms to counter disinformation and other online harms;
- understand the role of non-news and alternative media sources of disinformation; and
- identify the behavioural and psychological underpinnings of the spread of disinformation and other harmful content in the Canadian context.

The DCCP has also responded to the shifting disinformation environment through its

programming. In addition to its regularly updated program guidelines and calls for proposals, it launched two special calls for proposals to address mis- and disinformation related to COVID-19 in 2020, and one special call to address disinformation related to the Russian invasion of Ukraine in 2022.

The Government sees value in further coordination of such activities at the national level. A key stakeholder in the digital media literacy space, MediaSmarts, recently published a report advocating for a national digital media literacy strategy. The Government is considering this recommendation and how it may add value to the work already being done by the Government through the DCI and the DCCP.

Through the Canada Centre for Community Engagement and Prevention of Violence's Community Resilience Fund (CRF), the Government of Canada provides financial support to organizations working to improve Canada's understanding and capacity to prevent and counter violent extremism. The CRF has provided funding to programs aimed at developing media literacy programs to build resiliency to radicalization to violence. For example, the Institute for Strategic Dialogue is receiving CRF funding to partner with Montreal's Centre for the Prevention of Radicalization Leading to Violence to expand the 'Extreme Dialogue' project. This initiative is a free resource designed to be delivered by teachers, youth practitioners, social services and police, or young people themselves, by using films and supporting curriculum materials to learn about the true stories of those affected by violent extremism. This project aims to build resilience to radicalization leading to violence in youth by providing them with the knowledge, skills and values needed not only to openly discuss, but also challenge violent extremism in schools and communities.

As Canada's authority on cyber security and foreign signals intelligence, Communications Security Establishment (CSE) works in collaboration with partners across civil society and the private sector to strengthen Canada's cyber resilience through collaboration, innovation, and partnerships. For instance, *Get Cyber Safe* is a national public awareness campaign created to inform Canadians about cyber security and the steps they can take to stay safe online. CSE will continue to inform Canadians on modern threats and ways to protect themselves against them, including disinformation, misinformation and malinformation and welcomes any opportunity to develop new campaigns to promote cyber resilience.

Recommendation 31

That the Government of Canada continue to engage with academics, law enforcement and the public to increase awareness of IMVE and promote understanding across society of the threat posed by this form of violent extremism.

The Government agrees with this recommendation.

The Government of Canada recognizes that raising public awareness of IMVE threats and the Government's efforts to mitigate them is critical to ensuring Canadians' safety and security, and is committed to promoting transparency and civic engagement to counter IMVE.

In his December 2021 Mandate Letter, the Prime Minister asked the Minister of Public Safety to work with the Minister of Justice and Attorney General of Canada to bring forward measures to counter the rise of ideologically inspired violent extremism and strengthen the capacity of Canadian police and prosecutors to bring to justice cybercriminals and terror suspects to the fullest extent of the law. The Prime Minister also outlined his expectation to actively consider new ideas and issues as they arise, in part through public engagement, to work collaboratively toward a stronger and more resilient Canada. Engagement and outreach initiatives are routinely conducted by the security and intelligence community, including Public Safety Canada, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, and will remain a Government priority.

Within Public Safety Canada, the Canada Centre for Community Engagement and Prevention of Violence (the Canada Centre) leads the Government of Canada's efforts to counter radicalization to violence and aims to complement national security and criminal justice efforts, as well as broader initiatives to address harms like hate and gender-based violence. The Canada Centre leads the *National Strategy on Countering Radicalization to Violence* which highlights "Building, Sharing and Using Knowledge" as a priority. The Canada Centre funds research and the development of evidence-based resources through the Community Resilience Fund (CRF), which is the primary mechanism to support both preventative programming and research.

The CRF Call for Applications that concluded in January 2022 included as one of its priorities, "Locating harm, vulnerabilities and needs", to increase the evidence base about vulnerabilities, risks and pathways to violence, to better inform prevention efforts, including to address IMVE. Several proposals were received to help promote understanding about the nature and threats from IMVE, including to inform front-line practitioners such as social workers, mental health professionals and law enforcement. Additionally, the Canada Centre collaborates with leading national and international experts, which underscores the importance of supporting the still nascent field of prevention grow through cumulative learning. The Canada Centre's work involves routine engagement with communities on issues relevant to IMVE. Specific initiatives include: funding for local approaches for countering radicalization to violence and violent extremism; engagement with digital industry to address violent extremism and terrorist use of the Internet, as well as online hate; providing resources and training for front-line workers and practitioners, and; coordinating research to better understand radicalization and build an evidence base. The Canada Centre also coordinates the National Expert Committee on Countering Radicalization to Violence, which provides advice to the Minister of Public Safety on policies, programs and research priorities.

Public Safety Canada continues to enhance transparency and trust in Canada's national security apparatus through several consultative or advisory mechanisms. In 2021, Public Safety Canada's National Security Transparency Commitment Secretariat published the results of public opinion research in a report called, "National Security Information Sharing and Transparency Public Opinion Research". Eighty-three percent (83%) of respondents said that it was important that the Government of Canada provide information to Canadians about issues and threats related to terrorism and extremism, including IMVE. At the same time, only 20% of respondents

reported being knowledgeable of the national security threats facing Canada and Canadians.

The National Security Transparency Commitment (NSTC) Secretariat seeks to foster robust and open engagement between the Government of Canada and Canadians on a broad range of national security issues. Public Safety Canada launched the National Security Transparency Advisory Group (NS-TAG) in July 2019, which provides advice on how to implement the National Security Transparency Commitment. Composed of experts from academia, law enforcement and civil society, the NS-TAG is mandated to: infuse transparency into Canada's national security policies, programs and activities; increase public awareness, engagement and access to national security and related intelligence information; and promote transparency while ensuring the safety and security of Canadians. A diverse array of government and non-government experts attend each NS-TAG meeting as guest speakers to help inform the NS-TAG's advice, including the Director of CSIS, the Commissioner of the RCMP and the President of CBSA.

The NS-TAG has released three public reports to date on national security-related themes of its choosing, the first providing a general overview of Canada's national security environment and institutions. Its second report, *The Definition, Measurement, and Institutionalization of Transparency in National Security*, provided recommendations in support of stronger accountability and transparency mechanisms across national security departments and agencies. Its latest report published on May 31, 2022, *How National Security and Intelligence Institutions Engage with Racialized Communities*, takes note of the deep structural challenges that hinder effective community engagement and makes recommendations for how to address these challenges.

To foster deeper whole-of-society engagement, Public Safety Canada has spearheaded work to engage the public on the impact of national security threats on marginalized and vulnerable communities. Public Safety Canada hosted two web symposia in 2022 on islamophobia and anti-Asian hate, facilitating dialogue between Government and civil society on these issues. In addition, Public Safety Canada has launched training for the security and intelligence community and has commissioned public opinion research to bring awareness and greater insight to the differential impacts of national security on marginalized populations and increase cultural competency across a broad range of practitioners in this field.

Recommendation 32

That the Government of Canada consult with affected communities and law enforcement agencies to identify gaps in existing law and law enforcement regarding harmful online content, while upholding Charter rights.

The Government agrees with this recommendation.

The Government agrees that new legislation targeting online services should be informed by the views and experiences of affected communities, and that the concerns of law enforcement agencies in Canada should also inform decision-making in this area. With this in mind, the

Government continues to consult affected communities and law enforcement agencies in the development of a new legislative and regulatory framework for harmful content online.

Throughout these consultations, the Government continues to hear concerns that there is no legal framework to hold online services accountable for how they deal with harmful content online, and there are no effective avenues for affected users to properly flag and report harmful content.

The Government heard concerns that law enforcement is put at a disadvantage when some forms of content are removed and/or deleted by services. Law enforcement representatives noted that they require access to evidence, such as content and data, to investigate crimes. Law enforcement representatives noted that preservation of data enhances the ability of police to access that data when it is needed for criminal investigations. Furthermore, the removal of harmful content addresses symptoms and not causes. As such, the framework must be constructed in a way to reduce the harms associated with exposure to harmful content without interfering with the overarching priority of protecting Canadians from physical violence in the real world.

Some stakeholder groups expressed concern over privacy rights if data preservation and reporting to law enforcement are put in place. Those concerned with data preservation and reporting requirements cite the poor treatment of racialized and diaspora communities as the basis for their concerns, warning against potential for such requirements to result in over-reach and the undermining of Charter rights. On the other hand, historically marginalized communities are disproportionately the victims of online hate and IMVE content rather than the perpetrators.

The Government will continue to consult with both affected communities and law enforcement to develop a reasonable approach to filling gaps in Canada's legal framework when it comes to harmful content online and violence emanating from the online space.

The Royal Canadian Mounted Police (RCMP) continues to work with Public Safety Canada and security and intelligence partners on a strategic approach to address IMVE to ensure that the RCMP has both the resourcing and legislative tools required to effectively investigate IMVE threat actors in both the physical and online spaces. The RCMP continues to analyze legislative tools to determine to what extent modernization is required to meet the needs of investigators and analysts operating in the constantly evolving ideologically motivated threat landscape, particularly online.

Recommendation 33

That the Government of Canada invest in the development of Canada's cyber infrastructure, specifically to better identify and remove automated bots used to amplify extremist content accessible to Canadians online.

The Government takes note of this recommendation.

The Government of Canada is aware of the role that automated bots play in creating online echo chambers and amplifying certain types of content. As such, the Government is considering the role of automated bots used to amplify extremist content in the context of the Government's planned legislative and regulatory framework. In holding platforms accountable for the creation and spread of extremist content on their services, new legislation could compel platforms to assess and mitigate the malicious use of bots and bot networks in this context, where applicable, through regulation. Further examination will be needed to assess to what extent legislation could target bots or bot networks specifically.

The security and intelligence community works together with other government jurisdictions, small-and-medium enterprises, critical infrastructure owners and operators, and academia to raise Canada's cyber security broadly and to bring awareness to the type of manipulation that can be brought about by bots serving others' interests. As such, in the context of threats originating from overseas, the Communications Security Establishment will continue to work with partners in government and industry to combine our respective reach and authorities to tackle online threats so that Canada is a safe place for Canadians to live and work online.

Lastly, the Government recognizes the importance of civic digital literacy in addressing the creation, spread, and impact of online mis- and disinformation and has made it a priority to help equip Canadians with the tools and skills needed to critically assess online information. To that end, the Government funds digital literacy programs through the Department of Canadian Heritage's Digital Citizen Contribution Program (DCCP). Created in 2019, the DCCP has funded 46 projects with \$7 million to date to build citizen resilience to online disinformation across Canada through workshops, resources for educators, awareness activities, training tools, learning materials, and community outreach. These projects seek to build the critical and civic media consumption skills required to navigate the online information ecosystem for all Canadians. Digital literacy projects funded through the DCCP have resulted in 170 unique events and reach an average of 1.5 million Canadians.